by, acceptable to or approved by the government, should be utilized in evaluating potentially disqualifying and mitigating information fully and properly, and particularly for consultation with the individual's mental health care provider.

(b) *Conditions that could raise a security concern and may be disqualifying include:* (1) An opinion by a credentialed mental health professional that the individual has a condition or treatment that may indicate a defect in judgment, reliability, or stability;

(2) Information that suggests that an individual has failed to follow appropriate medical advice relating to treatment of a condition, e.g., failure to take prescribed medication;

(3) A pattern of high-risk, irresponsible, aggressive, anti-social or emotionally unstable behavior;

(4) Information that suggests that the individual's current behavior indicates a defect in his or her judgment or reliability.

(c) *Conditions that could mitigate security concerns include:* (1) There is no indication of a current problem;

(2) Recent opinion by a credentialed mental health professional that an individual's previous emotional, mental, or personality disorder is cured, under control or in remission and has a low probability of recurrence or exacerbation;

(3) The past emotional instability was a temporary condition (e.g., one caused by a death, illness, or marital breakup), the situation has been resolved, and the individual is no longer emotionally unstable.

§ 147.12 Guideline J—Criminal conduct.

(a) *The concern.* A history or pattern of criminal activity creates doubt about a person's judgment, reliability and trustworthiness.

(b) *Conditions that could raise a security concern and may be disqualifying include:* (1) Allegations or admissions of criminal conduct, regardless of whether the person was formally charged;

(2) A single serious crime or multiple lesser offenses.

(c) *Conditions that could mitigate security concerns include:* (1) The criminal behavior was not recent;

(2) The crime was an isolated incident;

(3) The person was pressured or coerced into committing the act and those pressures are no longer present in that person's life;

(4) The person did not voluntarily commit the act and/or the factors leading to the violation are not likely to recur;

(5) Acquittal;

(6) There is clear evidence of successful rehabilitation.

§ 147.13 Guideline K—Security violations.

(a) *The concern.* Noncompliance with security regulations raises doubt about an individual's trustworthiness, willingness, and ability to safeguard classified information.

(b) *Conditions that could raise a security concern and may be disqualifying include.* (1) Unauthorized disclosure of classified information;

(2) Violations that are deliberate or multiple or due to negligence.

(c) *Conditions that could mitigate security concerns include actions that:* (1) Were inadvertent;

(2) Were isolated or infrequent;

(3) Were due to improper or inadequate training;

(4) Demonstrate a positive attitude towards the discharge of security responsibilities.

§ 147.14 Guideline L—Outside activities.

(a) *The concern.* Involvement in certain types of outside employment or activities is of security concern if it poses a conflict with an individual's security responsibilities and could create an increased risk of unauthorized disclosure of classified information.

(b) *Conditions that could raise a security concern and may be disqualifying include any service, whether compensated, volunteer, or employment with:* (1) A foreign country;

(2) Any foreign national;

(3) A representative of any foreign interest;

(4) Any foreign, domestic, or international organization or person engaged in analysis, discussion, or publication of material on intelligence, defense, foreign affairs, or protected technology.

(c) *Conditions that could mitigate security concerns include:* (1) Evaluation of the outside employment or activity indicates that it does not pose a conflict with an individual's security responsibilities;

(2) The individual terminates the employment or discontinues the activity upon being notified that it is in conflict with his or her security responsibilities.

§ 147.15 Guideline M—Misuse of Information technology systems.

(a) *The concern.* Noncompliance with rules, procedures, guidelines, or regulations pertaining to information technology systems may raise security concerns about an individual's trustworthiness, willingness, and ability to properly protect classified systems, networks, and information. Information Technology Systems include all related equipment used for the communication, transmission, processing, manipulation, and storage of classified or sensitive information.

(b) *Conditions that could raise a security concern and may be disqualifying include:* (1) Illegal or unauthorized entry into any information technology system;

(2) Illegal or unauthorized modification, destruction, manipulation or denial of access to information residing on an information technology system;

(3) Removal (or use) of hardware, software, or media from any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations;

(4) Introduction of hardware, software, or media into any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations.

(c) *Conditions that could mitigate security concerns include:* (1) The misuse was not recent or significant;

(2) The conduct was unintentional or inadvertent;

(3) The introduction or removal of media was authorized;

(4) The misuse was an isolated event;

(5) The misuse was followed by a prompt, good faith effort to correct the situation.

Subpart B—Investigative Standards

§ 147.18 Introduction.

The following investigative standards are established for all United States Government civilian and military personnel, consultants, contractors, employees of contractors, licensees, certificate holders or grantees and their employees and other individuals who require access to classified information, to include Sensitive Compartmented Information and Special Access Programs, and are to be used by government departments and agencies as the investigative basis for final clearance determinations. However, nothing in these standards prohibits an agency from using any lawful investigative procedures in addition to these requirements in order to resolve any issue identified in the course of a background investigation or reinvestigation.

§ 147.19 The three standards.

There are three standards (Attachment D to this subpart part summarizes when to use each one):

(a) The investigation and reinvestigation standards for ''L'' access authorizations and for access to confidential and secret (including all secret-level Special Access Programs not specifically approved for enhanced investigative requirements by an official authorized to establish Special Access Programs by section in 4.4 of Executive Order 12958) (60 FR 19825, 3 CFR 1995 Comp., p. 33);

(b) The investigation standard for''Q'' access authorizations and for access to top secret (including top secret Special Access Programs) and Sensitive Compartmented Information;

(c) The reinvestigation standard for continued access to the levels listed in paragraph (b) of this section.